

**This Page Is Inserted by IFW Operations
and is not a part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

AU 00 / 351
Sertifikaat

REPUBLIEK VAN SUID-AFRIKA

Certificate

PATENTKANTOOR

PATENT OFFICE

DEPARTEMENT VAN HANDEL
EN NYWERHEID

REPUBLIC OF SOUTH AFRICA

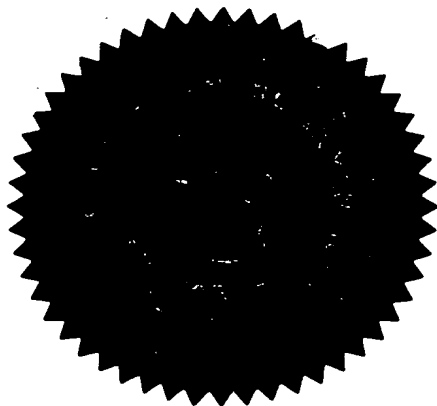
DEPARTMENT OF TRADE
AND INDUSTRYHiermee word gesertifiseer dat
This is to certify that

this is a true copy of the provisional specification filed in support of South African Patent Application No. 99/2823 entitled METHOD OF AND SYSTEM FOR CONTROLLING A BLASTING NETWORK on 20 APRIL 1999.

REC'D 30 JUN 2000

WIPO

PCT

**PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)Geteken te
Signed at

PRETORIA

in die Republiek van Suid-Afrika, hierdie
in the Republic of South Africa, this4th dag van
day of

May 2000

Registrateur van Patente
Registrar of Patents

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978

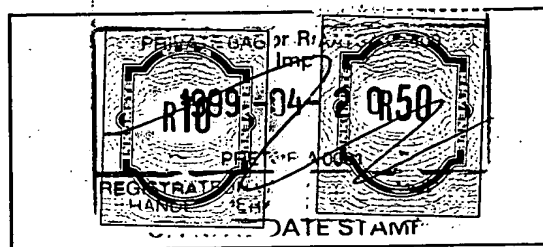
APPLICATION FOR A PATENT AND ACKNOWLEDGEMENT OF
RECEIPT

(Section 30(1) - Regulation 22)

The grant of a patent is hereby requested by the undermentioned applicant on the basis of the present application filed in duplicate

OFFICIAL APPLICATION NO.

21	01	992823
----	----	--------



FULL NAME(S) OF APPLICANT(S)

71	EXPERT EXPLOSIVES (PROPRIETARY) LIMITED
----	---

ADDRESS(ES) OF APPLICANT(S)

1 Nobel Avenue, Modderfontein, 1645	
-------------------------------------	--

TITLE OF INVENTION

54	METHOD OF AND SYSTEM FOR CONTROLLING A BLASTING NETWORK
----	---

Priority is claimed as set out on the accompanying Form P2.

The earliest priority claimed is : NONE

This application is a patent of addition to Patent Application No.	21	01	
--	----	----	--

This application is a fresh application in terms of section 37 and based on Application No.	21	01	
---	----	----	--

THIS APPLICATION IS ACCOMPANIED BY:

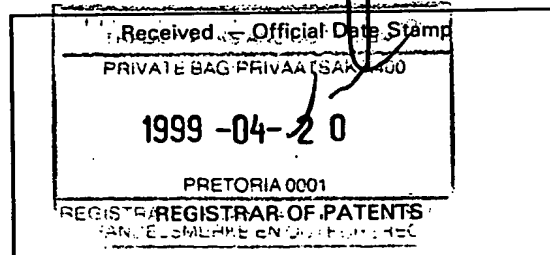
- | | | |
|-------------------------------------|----|--|
| <input checked="" type="checkbox"/> | 1 | A single copy of a provisional specification of13..... pages |
| <input type="checkbox"/> | 2 | Two copies of a complete specification of pages |
| <input checked="" type="checkbox"/> | 3 |3..... sheets of Informal Drawings |
| <input type="checkbox"/> | 4 | sheets of Formal Drawings |
| <input type="checkbox"/> | 5 | Publication particulars and abstract (Form P8 in duplicate) |
| <input type="checkbox"/> | 6 | A copy of Figure of drawings (if any) for the abstract |
| <input type="checkbox"/> | 7 | Assignment of Invention |
| <input type="checkbox"/> | 8 | Certified priority document(s) Number(s) |
| <input type="checkbox"/> | 9 | Translation of priority document(s) |
| <input type="checkbox"/> | 10 | An assignment of priority rights |
| <input type="checkbox"/> | 11 | A copy of the Form P2 and the specification of SA Patent Application |
| <input type="checkbox"/> | 12 | A declaration and power of attorney on Form P3 |
| <input type="checkbox"/> | 13 | Request for ante-dating on Form P4 |
| <input type="checkbox"/> | 14 | Request for classification on Form P9 |
| <input checked="" type="checkbox"/> | 15 | Form P2 in duplicate |

21	01	
----	----	--

74	ADDRESS FOR SERVICE: McCALLUM, RADEMEYER & FREIMOND, Maclyn House, June Avenue, Bordeaux P.O. Box 1130, Randburg, 2125
----	---

Dated this 20th day of APRIL 1999

.....
McCALLUM, RADEMEYER & FREIMOND
PATENT AGENTS FOR APPLICANT(S)



REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978

PROVISIONAL SPECIFICATION

(Section 30(1) - Regulation 27)

OFFICIAL APPLICATION NO

21	01	992823
----	----	--------

LODGING DATE

22	20 APRIL 1999
----	---------------

FULL NAME(S) OF APPLICANT(S)

71	EXPERT EXPLOSIVES (PROPRIETARY) LIMITED
----	---

FULL NAME(S) OF INVENTOR(S)

72	LIVIA DRAGNE; VIVIAN EDWARD PATZ; CHRISTIAAN HOOGENBOEZEM
----	---

TITLE OF INVENTION

54	METHOD OF AND SYSTEM FOR CONTROLLING A BLASTING NETWORK
----	---

BACKGROUND OF THE INVENTION

5 This invention relates generally to a blasting network and to a method of controlling the operation thereof.

10 For safety reasons a blast controlling system used for remotely controlling a blasting network has traditionally been isolated from other networks at a blasting site e.g. at a mine. The data on the blasting system can however be used to monitor productivity, implement stock control and improve mining methods by making blast information available to those who need such information. It is also possible to schedule and initiate blasts from a central control facility through a
15 suitable blast controlling system.

Another possibility which arises particularly due to the fact that computers are being used as top level system controllers for distributed networks of blasters is to make use of a computer network using Internet or Intranet capabilities.

20 There are however inherent risks associated with Internet connections. Chief of these is the risk that a hacker or unauthorised user may penetrate the system and deliberately or inadvertently generate an unsafe or dangerous command which can arm and fire the blasting system. This type of action can have catastrophic results.

5

SUMMARY OF THE INVENTION

10

The invention provides a method of controlling a blasting network which includes the steps of designating at least one unsafe message, placing a communication line to the network in a control mode, monitoring the communication line for the unsafe message, and preventing the unsafe message, when detected, from reaching the blasting network.

15

The unsafe message may be prevented from reaching the blasting network simply by ignoring the message and not allowing its onward transmission. Alternatively the unsafe message may be scrambled so that it is no longer in an unsafe form.

20

"Unsafe message", as used herein, is used to designate a message or command which, if received by the blasting network, could result in unwanted or adverse conditions or consequences. For example arm and fire commands, if received by the blasting network at an unwanted time, could cause a blast to be initiated in the presence of personnel and thereby result in death or injury.

25

Preferably therefore the method of the invention includes the step of designating at least two unsafe messages which respectively are equated with arm and fire commands.

5 The method may include the steps of placing the communication link in an operational mode and, when an unsafe message is detected, of allowing the unsafe message to reach the blasting network.

10 Unsafe messages may be categorised as legal or illegal. The latter group of messages includes those which are illegally generated, for example those messages which arise from any source other than a control unit connected to the communication link. Legal messages are then those which are generated by the control unit.

15 Unsafe messages generated by the control unit may initially be scrambled. In this instance it falls within the scope of the method of the invention, when a legal unsafe message is generated in scrambled form, and the communication line is in an operational mode, to unscramble a scrambled unsafe message, when detected, and then to transmit the unscrambled unsafe message to the blasting network.

20

25 The invention also provides a system for controlling a blasting network which includes means for placing a communication line to the network in a control mode, means for monitoring the communication line for at least one previously designated unsafe message, and means for preventing the unsafe message, when detected, from reaching the blasting network.

5 The unsafe message, when detected, may be ignored or it may be scrambled so that it is placed in a safe condition.

10 The communication line may be connected to a control unit which is capable of generating legal unsafe messages and the system may then include means for placing the communication line in an operational mode and means for unscrambling a legal scrambled unsafe message, when detected, into an unscrambled form and then for transmitting the unscrambled unsafe message to the blasting network.

15 BRIEF DESCRIPTION OF THE DRAWINGS

The invention is further described by way of examples with reference to the accompanying drawings in which:

20 Figure 1 is a block diagram of an electronic blasting system according to the invention,

Figure 2 is a block diagram of a communication fire wall for use in the system of Figure 1,

Figure 3 is a logical flowchart of the operation of a filter, used in the system of Figure 1, according to a first form of the invention, and

25 Figure 4 is a flowchart similar to that shown in Figure 3 for a variation of the invention.

5 DESCRIPTION OF PREFERRED EMBODIMENT

When a blasting system is connected to an Intranet or Internet facility, access is provided to information stored in a data base associated with the blasting system. This information is useful inter alia to managers, personnel involved in stores and production, seismic monitoring installations, logistical control units, etc.

10 A perceived risk with a connection of the aforementioned kind is that unauthorised users may hack through the network security to tamper with the blasting system which is a safety critical system. An unanticipated system fault may result in the safety of the system being compromised and this may lead to the blasting system being fired prematurely which can cause injury or fatalities.

15 Modern networks provide high levels of user security but due to the complexities of such systems it is not always possible to carry out a complete exhaustive safety analysis of the control software, operating systems and associated fire walls.

20 Figure 1 of the accompanying drawings illustrates in block diagram form a system which allows an Internet or Intranet connection to be made to a blasting network with improved safety.

5 The system includes an Internet or Intranet facility or connection arrangement 10, a blasting controller or control computer 12 which is used to control and activate blasts remotely, a communication fire wall 14, a blasting network 16, and a variety of interrogating terminals 18.

10 The blasting controller 12 is used in a known manner and includes a standard device employed to control the network 16 and to activate the initiation thereof, remotely. These aspects are known in the art and hence are not further described herein. Similarly the blasting network 16 consists of an assembly of detonators and communication devices installed in a known manner at a blasting
15 site, making use of known technology.

The communication fire wall includes a locking device 18 for placing a communication line 20 to the blasting network in a control mode, or in an operational mode, according to requirement. As used herein the expression
20 "locking device" includes any switchable component or mechanism which allows the fire wall to be made operational, or to be rendered inoperational, according to requirement. The locking device may be operated using a key, by means of an electronic keypad requiring a password, or it may be a remotely activated switch on a private connection. Thus, in a general sense, the locking device may
25 be mechanically or electronically operated.

5 The remote terminals 18 may vary according to requirement. The terminals may
for example provide access, via an Internet connection, to the blasting network
for managers 18A, stock controllers 18B, or a seismic monitoring unit 18C.
These examples are merely illustrative and are not limiting.

10 Figure 2 illustrates further detail of the communication fire wall 14. The filter
includes communication interfaces 22 and 24 which allow communication to take
place with the communication line 20, an electronic filter 26 and, in this example,
a locking device 18 which consists of a mechanical or electronic switch 28 which
is activated by means of a mechanical or electronic key 30.

15 The operation of the electronic filter 26 is described hereinafter with reference
to Figure 3 and a variation of such operation is described with reference to
Figure 4.

20 As indicated, by connecting the blasting system 16 to the Internet 10 a potential
safety risk is introduced due to the possibility being created that hackers can
penetrate the system. This risk is eliminated by making use of the
communication fire wall 14 to filter out unsafe or dangerous commands like arm,
which results in the blasting network being armed, and fire which causes the
25 blasting network to be initiated.

5 It is to be noted that the communication medium and protocols used to communicate between the blast controlling system and the blasting network may be of any appropriate type capable of achieving reliable communication.

10 The communication interfaces allow the communication to interface with the electronic components incorporated in the filter 26. These electronic components may include a micro controller, programmable logic devices or discrete components. The choice of the electronic components is determined inter alia by the complexity of the communication protocol which is used.

15 Data on the line 20 (block 32) is input to the filter 26. The filter waits for communication (34) and reads each message on the line (36). If a message is unsuccessfully read then the system returns to the mode at which it awaits communication.

20 Once a message is successfully read (block 38) a test is carried out to see if the filter 26 has been activated (step 40). As noted the filter is activated by means of the mechanical key 30. When the filter is activated it is capable of transmitting unsafe or dangerous messages, such as arm and fire commands, which have been legally generated by means of the blasting computer 12, to the blasting network 16. Thus if the filter has been activated (step 42) any message received, regardless of its origin, is collected (block 44) and transmitted via the

25

5 communication interface 24 as output data (46). The system then reverts to its waiting mode at which further messages are awaited.

10 On the other hand if the filter is not activated then any message received is tested to see whether it is safe or unsafe (step 48). Safe messages are collected and transmitted on the communication line (steps 44 and 46). If an unsafe message is detected then it is assumed that this has been illegally generated and the message is collected but simply ignored (step 50). The system then reverts to the mode at which it waits for further communication.

15 If an unsafe or dangerous command is detected then an alarm signal, visual or audible, is generated. A count is also kept of the number of dangerous messages detected.

20 With the control steps shown in Figure 3 the logic is such that dangerous commands which are generated when the filter is in a safe mode are assumed to be illegally generated and are ignored. Other messages are transmitted to the required destination. The system thus possesses the facility for allowing data associated with the blast network to be accessed from the remote points 18. The data may be located at the blasting controller 12 or at the blasting network 16.

25 It is however not possible to transmit an unsafe command to the network 16 unless the filter 26 has been placed in an unsafe state i.e. unless the filter has

5 been activated.

10 In the logical sequence shown in Figure 4 many of the steps are similar or identical to corresponding steps in the sequence shown in Figure 3 and consequently bear the same reference numerals. The flowchart shown in Figure 4 is however intended for use with a blasting controller 12 which scrambles dangerous commands. Thus legally generated arm and fire commands, produced by the controller 12, are transmitted to the blasting network 16 in a scrambled state.

15 In the step 40 a test is carried out to see if the filter 26 is activated or deactivated. In the latter case a test is then carried out on the received message to see whether it contains an unsafe or dangerous command such as fire or arm (step 52). If the command is unsafe then, in step 54, the command is scrambled whereafter the scrambled command is collected and transmitted (steps 44 and 20 46).

 On the other hand if the received message is safe then no scrambling takes place and the message is transmitted in an unscrambled form to its destination.

25 If the filter has not been deactivated then, in step 56, a test is carried out to determine whether the received message is safe or unsafe. If the message is

5 unsafe then the received message will be a scrambled fire or arm command.
The scrambled message is unscrambled (step 58) and is then transmitted to its
destination. If the message is not a scrambled unsafe message then, in step 52,
a test is carried out to see if the message is an unsafe message in unscrambled
10 form. If the test result is affirmative then it is assumed that the message has
been illegally generated and, as before, the message is scrambled (step 54)
before being transmitted. If the test result is negative then the message is
transmitted in the received form to its destination.

15 It follows that the locking device 18 is used to bypass the filter when it is safe to
blast. The bypass is achieved by hard wiring the communication around the filter
or by the filter sensing the status of the switch and then, based on the status,
filtering the dangerous commands out or unscrambling them.

20 If the filter has sufficient intelligence then it can send the arm and fire command.
It would therefore not be possible for an unauthorised user to initiate a blast.
This could only be achieved by activating the fire wall via the mechanical or
locking device 18.

25 The control computer 12 may communicate directly with the filter 26. If there is
no response from the filter then the control computer will not attempt
communication with the blasting network. The filter can thus act as a software

5 dongle. If, as is the case with the Figure 4 embodiment, dangerous legal
messages are scrambled then the filter must be installed for the system to
operate.

10 It is to be noted that normal commands to query the blasting network and to
determine the status of components at the blasting site are unaffected. Once the
blast area is clear the mechanical or electrical key is used to disable the filtering
action and unblock the commands. The arm and fire commands may now be
sent through the filter via the blast network to the blasting equipment. The
control computer will scramble the dangerous commands. The filter, when
15 unblocked, will correct the scrambled commands. If the filter is not present the
scrambled dangerous commands will be sent to the blasting network. The
blasting network will discard these commands.

DATED this 20th day of APRIL 1999

20

McCALLUM, RADEMEYER & FREIMOND
Patent Agents for the Applicant

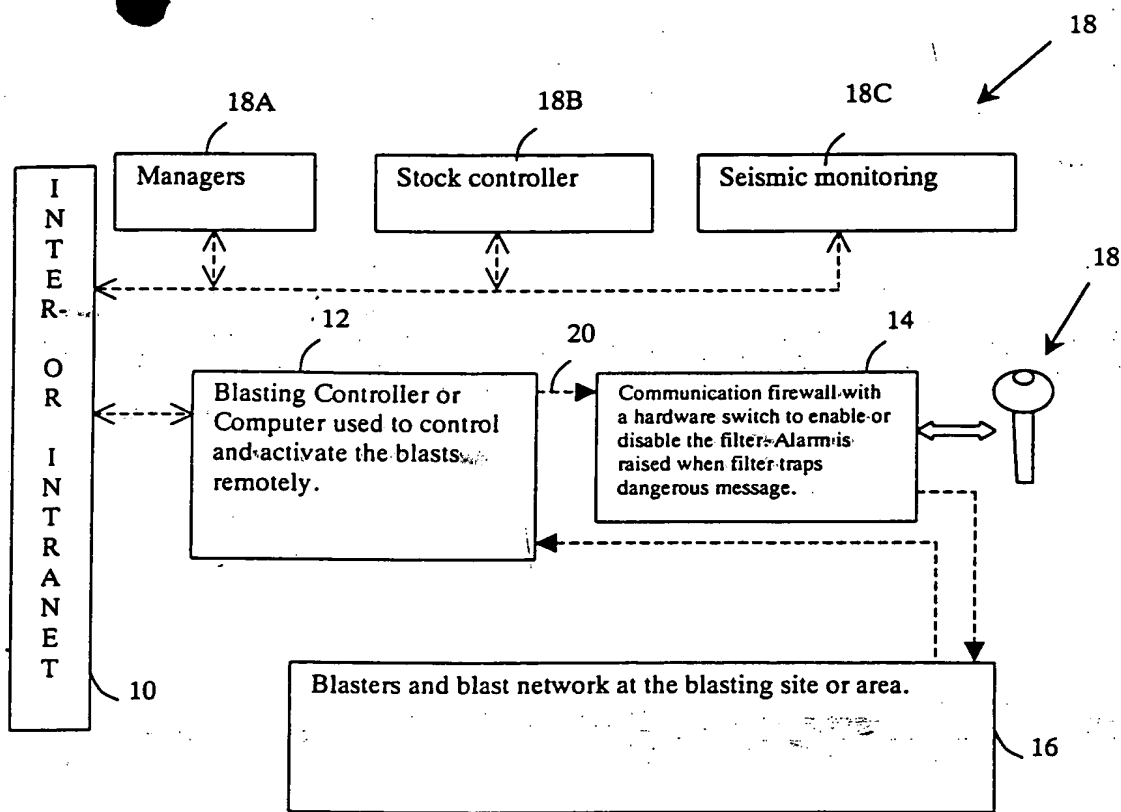


Fig 1

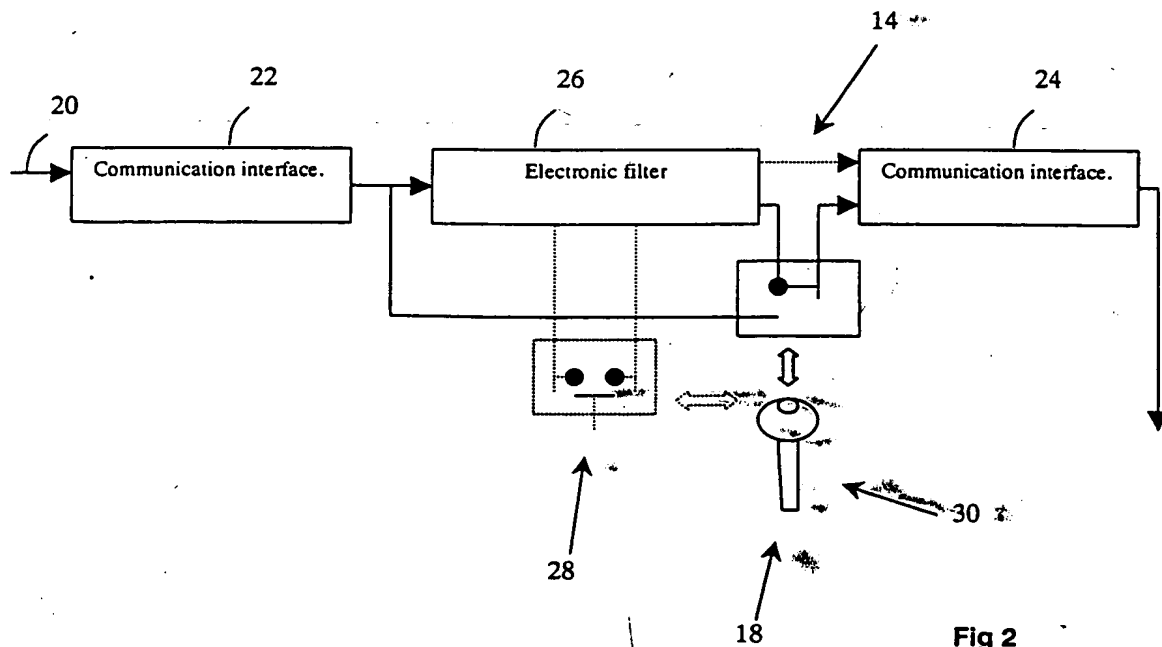


Fig 2

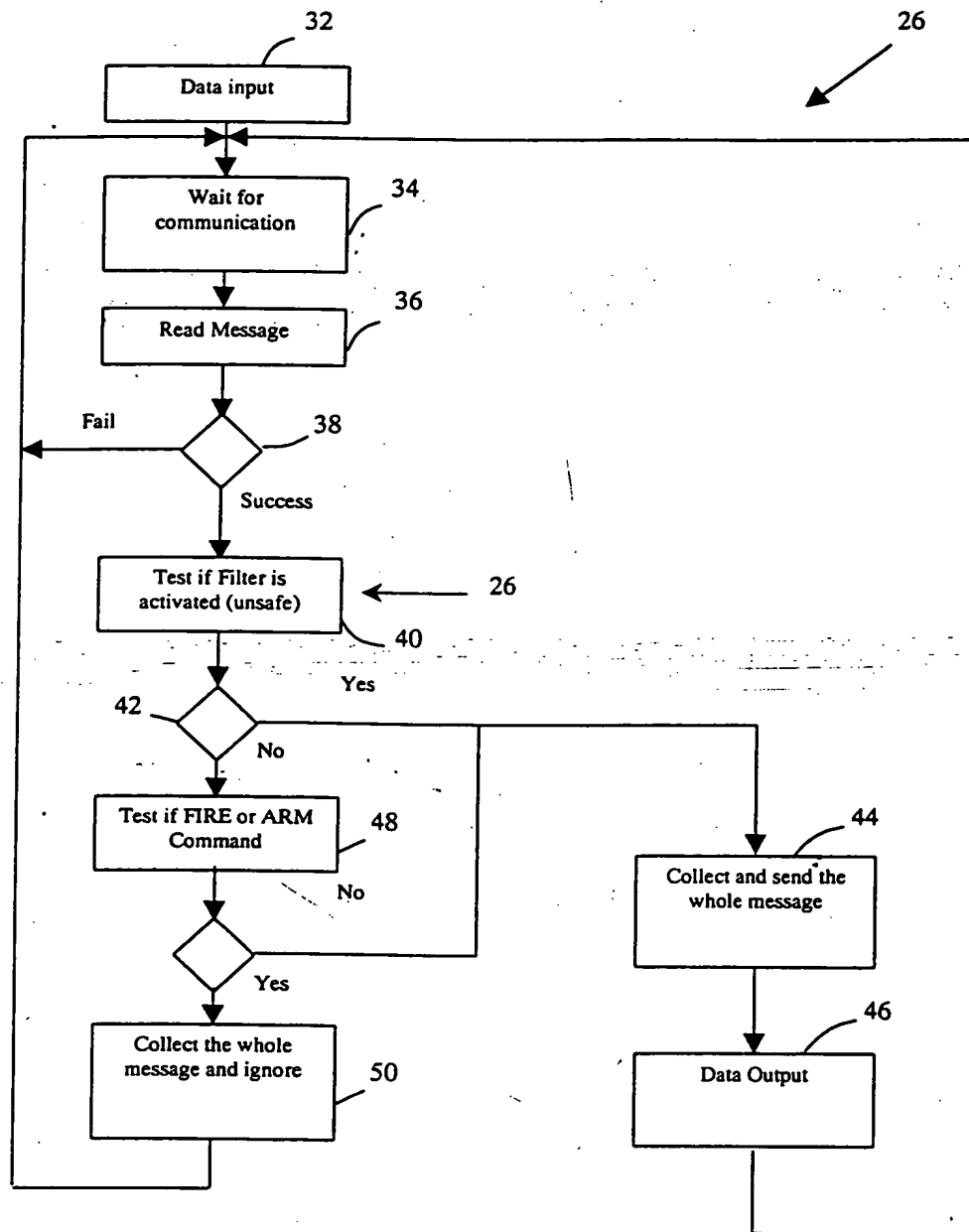


Fig 3

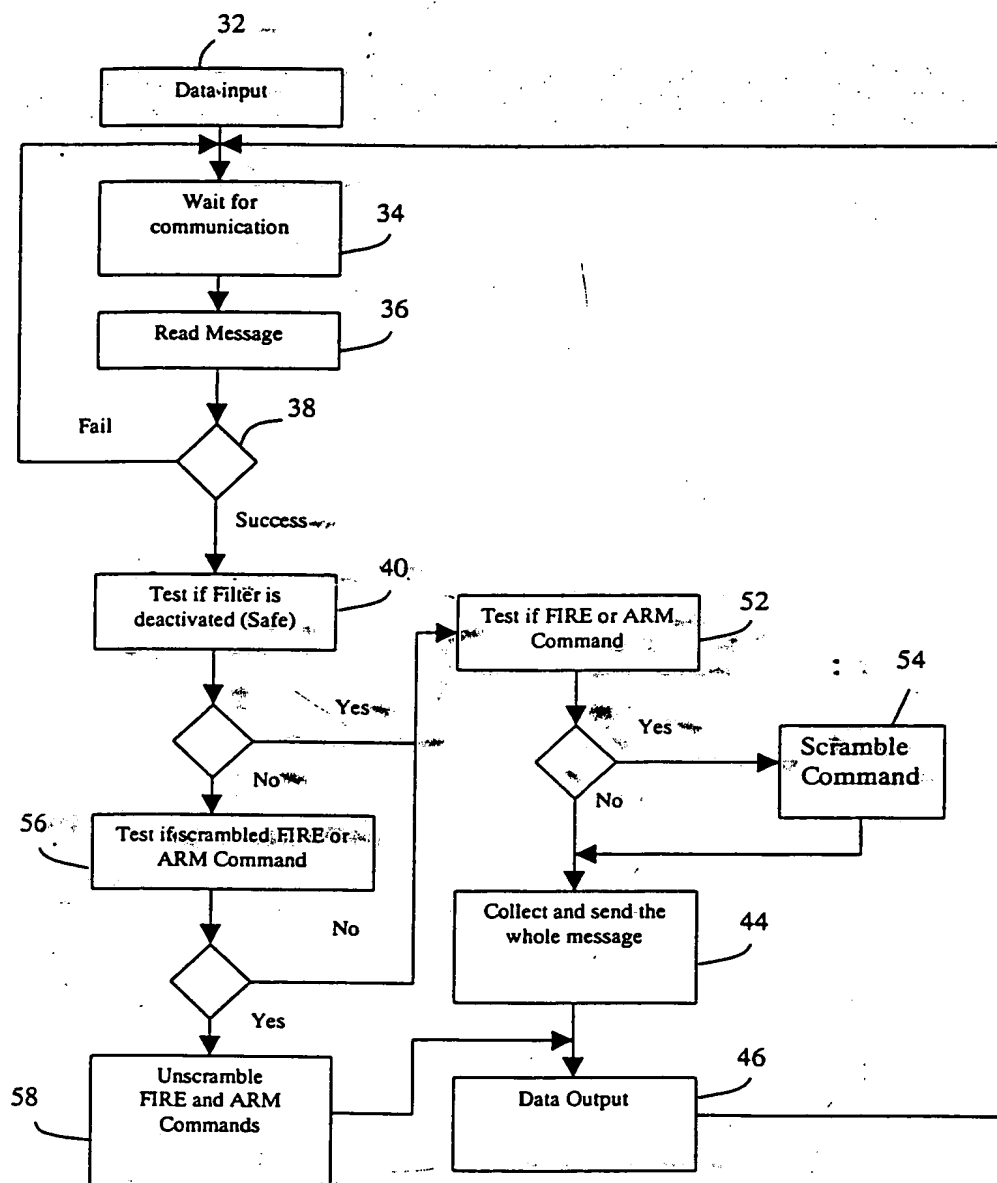


Fig 4